(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許出願公告番号

特公平7－87237

(24)(44)公告日　平成７年(1995)９月20日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０１Ｌ 27/04				
21/82				
21/822				
			Ｈ０１Ｌ 27/ 04	Ａ
			29/ 78	３７１

請求項の数５(全 11 頁)　最終頁に続く

(21)出願番号　特願平2－4397

(22)出願日　平成２年(1990)１月11日

(65)公開番号　特開平2－232960

(43)公開日　平成２年(1990)９月14日

(31)優先権主張番号　２９７４７２

(32)優先日　1989年１月12日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　999999999
ジェネラル・インストルメント・コーポレーション
アメリカ合衆国、ニューヨーク州、10153　ニューヨーク、フィフス・アベニュー　767

(72)発明者　ロバート・シー・ギルバーグ
アメリカ合衆国、カリフォルニア州　92131、サンデイエゴ、カミニート・ガルシア　11484

(72)発明者　リチャード・エム・ノウルズ
アメリカ合衆国、カリフォルニア州　92126、サンデイエゴ、ヘンプヒルウエイ　10323

(74)代理人　弁理士　鈴江　武彦　(外３名)

審査官　小野田　誠

最終頁に続く

(54)【発明の名称】　集積回路チップ

【特許請求の範囲】

【請求項１】保護データが処理および／または記憶される保護領域（11）を有する集積回路チップ（10）であり、

回路要素部品を形成する拡散部品（S,D）を有する半導体層（SC）と；

前記部品を相互に接続して保護データを配分、記憶、処理および／またはその処理を実行させるための、マイクロプロセッサ（14），データバス（16），アドレスバス（17），転送論理回路（18），クロック並びにパワー制御回路（20）及び複数のメモリ（M_1,M_2…M_n）からなる複数の回路要素，を形成するように前記半導体層と結合される第１導電層（CN_1）と；

前記回路要素を上から覆って、前記回路要素を外部から検知出来ない様にシールドする前記保護領域（11）を形成すると共に、前記回路要素の意図された機能に対し必要な所定の信号を前記回路要素に伝えるために前記回路要素と接続される第２導電層（CN_2）であり、前記保護領域に記憶され或るいはそこで処理されるデータを検知および／または修正出来る様にする為に前記第２導電層を除去すれば、前記必要な所定の信号が前記回路要素へ送られることが妨げられ、従って前記回路要素の意図された機能が阻まれる事となる、前記第２導電層と；を具備し、

クロック信号を発生させ且つ保護データを記憶および／または処理するシールドされた、前記回路要素の内のマイクロプロセッサ（14）及び複数のメモリ（M_1,M_2…M_n）に前記クロック信号を供給する手段（20）を有する前記集積回路チップ（10）。

【請求項２】前記所定の信号がパワー信号であり、前記

集積回路チップが非保護データと制御信号とを処理および／または記憶する非保護領域（12）をさらに具備し、前記シールドされた回路要素が、非保護データおよび／または制御信号を前記保護領域（11）と前記非保護領域（12）間で転送する事を可能にする為の、前記パワー信号で付勢される前記論理回路（18）を有する請求項（１）記載の集積回路チップ（10）。

【請求項３】前記第１導電層の前記シールドされた回路要素が保護データを記憶するための複数のメモリ（M_1,M_2…M_n）と前記メモリにデータを記憶させる様に出来る論理回路（14）とを有し、前記第２導電層（CN_2）は前記論理回路を機能させる事が出来るのに必要な信号を伝える様に適合され、その結果前記第２導電層を前記の様に除去すれば、データが前記メモリに記憶される事が妨げられる請求項（１）記載の集積回路チップ（10）。

【請求項４】保護データが処理および／または記憶される保護領域（11）を有する集積回路チップ（10）であり、

回路要素部品を形成する拡散部品（S,D）を有する半導体層（SC）と；

前記部品を相互に接続して保護データを配分、記憶、処理および／またはその処理を実行させるための、マイクロプロセッサ（14），データバス（16），アドレスバス（17），転送論理回路（18），クロック並びにパワー制御回路（20）及び複数のメモリ（M_1,M_2…M_n）からなる複数の回路要素，を形成するように前記半導体層と結合される第１導電層（CN_1）と；

前記回路要素を上から覆って、前記回路要素を外部から検知出来ない様にシールドする前記保護領域（11）を形成すると共に、前記回路要素の意図された機能に対し必要な所定の信号を前記回路要素に伝えるために前記回路要素と接続される第２導電層（CN_2）であり、前記保護領域に記憶され或るいはそこで処理されるデータを検知および／または修正出来る様にする為に前記第２導電層を除去すれば、前記必要な所定の信号が前記回路要素へ送られることが妨げられ、従って前記回路要素の意図された機能が阻まれる事となる、前記第２導電層と；を具備し、

前記所定の信号がパワー信号であり、前記集積回路チップが非保護データと制御信号とを処理および／または記憶する非保護領域（12）をさらに具備し、前記シールドされた回路要素が非保護データおよび／または制御信号を前記保護領域（11）と前記非保護領域（12）間で転送する事を可能にする為の、前記パワー信号で付勢される前記論理回路要素（18）を有する前記集積回路チップ（10）。

【請求項５】保護データが処理および／または記憶される保護領域（11）を有する集積回路チップ（10）であり、

回路要素部品を形成する拡散部品（S,D）を有する半導体層（SC）と；

前記部品を相互に接続して保護データを配分、記憶、処理および／またはその処理を実行させるための、マイクロプロセッサ（14），データバス（16），アドレスバス（17），転送論理回路（18），クロック並びにパワー制御回路（20）及び複数のメモリ（M_1,M_2…M_n）からなる複数の回路要素，を形成するように前記半導体層と結合される第１導電層（CN_1）と；

前記回路要素を上から覆って、前記回路要素を外部から検知出来ない様にシールドする前記保護領域（11）を形成すると共に、前記回路要素の意図された機能に対し必要な所定の信号を前記回路要素に伝えるために前記回路要素と接続される第２導電層（CN_2）であり、前記保護領域に記憶され或るいはそこで処理されるデータを検知および／または修正出来る様にする為に前記第２導電層を除去すれば、前記必要な所定の信号が前記回路要素へ送られることが妨げられ、従って前記回路要素の意図された機能が阻まれる事となる、前記第２導電層と；を具備し、

前記第１導電層の前記シールドされた回路要素が保護データを記憶するための複数のメモリ（M_1,M_2…M_n）と前記メモリにデータを記憶させる様に出来る論理回路（14）とを有し、前記第２導電層（CN_2）は前記論理回路を機能させる事が出来るのに必要な信号を伝える様に適合され、その結果前記第２導電層を前記の様に除去すれば、データが前記メモリに記憶される事が妨げられる前記集積回路チップ（10）。

【発明の詳細な説明】

［発明の目的］

（産業上の利用分野）

本発明は一般に電子的データの処理システム用集積回路チップに関し、特に集積回路チップの保護領域で記憶されたり処理される保護データの検知や修正を防止することに向けられている。

（従来の技術）

保護データを処理し記憶する集積回路チップは保護データを処理し記憶する回路要素をもった保護領域と、非保護データと制御信号を処理し記憶する回路要素を持つ非保護領域とを備えている。集積回路チップは回路要素部品を形成する拡散部を有する半導体層と、回路要素を形成する部品を内部接続するために前記半導体層と接続された第１導電層とを具備する。すべての現在の集積回路チップは通常回路要素と部品を相互接続するために１つ或はそれ以上の導電層を有する。一般的にこれ等の層は制御信号とパワー信号両者を伝えるのに使われ、信号の相互接続の密度を最大とし、そのような相互接続に必要な面積を減少させることを目標としている。

この保護領域は更に、保護領域内にあるデータ処理回路要素により保護データを処理するために保護領域内のデータバスへ非保護データと制御信号を転送する回路要素

を有する。保護領域内の論理回路要素は非保護データと制御信号を非保護領域と保護領域内のデータバス間に保護領域内のデータ処理回路要素により発生された制御信号に応じて転送することができる。

（発明が解決しようとする課題）

それにも拘らず、たとえこのような集積回路チップで保護データが保護領域から非保護領域へ容易に転送され得ないとしても、保護領域内に記憶されたか或いは処理中の保護データに例えば走査形電子顕微鏡（SEM）或いは顕微鏡に接続されたプローブのような診断装置を使った検査によりそこから保護データにアクセス出来る保護領域内の与えられたノードに対しアクセスをすることができる。又特定の制御信号をプローブのような手段で保護領域内の論理回路要素に送ることにより、論理回路が保護データを保護領域内のデータ処理回路要素により処理するために非保護と保護両データを伝達する保護領域内のデータバスから非保護領域へ転送することをさせることが或は保護領域内に記憶された保護データはチップの所望の保護を危くされることが出来るかもしれない悪意のある内密のデータによりおきかえられることが出来得る。

［発明の構成］

（課題を解決するための手段）

この発明は、回路要素部品を形成する拡散部品を有する半導体層と、保護データを配分、記憶、処理および／またはその処理を実行させるための回路要素を形成する要素相互を接続するように半導体層と結合される第１導電層と、回路要素を上から覆って、その回路要素を外部から検知出来ない様にシールドする保護領域を形成すると共にこの回路要素の意図された機能に対し必要な所定の信号を回路要素に伝える為に回路要素に接続される第２導電層であり、この保護領域に記憶される或いはそこで処理されるデータを検知および／または修正出来る様にする為にこの第２導電層を除去すると所定の必要な信号が回路要素へ送られなくなり、従って意図した機能が行えなくなるような、保護データが処理および／または記憶される保護領域を有する集積回路チップを提供する。

この発明の一態様においては、前記所定の信号がパワー信号である。本発明のこの態様に係わる一実施例においては、前記第１の導電層のシールドされた回路要素が保護データを記憶するための揮発性ランダムアクセスメモリ（RAM）の如き揮発性メモリを有し、このメモリは所定のパワー信号で動かされ、この結果、メモリの検知を可能にする第２の導電層の除去はパワーがメモリから遮断されることになるであろう。メモリが揮発性であるから、これからパワーを遮断することはメモリに記憶されている保護データを消去することになる。

前記一実施例において、第１導電層内のそのような複数の揮発性メモリが夫々個別に、夫々のメモリと第２導電層の重った場所のみから所定のパワー信号を受けられるようにそのメモリと重った第２導電層のその場所のみと接続され、この結果、メモリを検知するためにメモリを覆っている第２の導電層のそれらの部分のみを除去することは、この除去により露出したメモリからパワーが遮断されるので、無益となるであろう。

この発明に係わる非保護データと制御信号が処理および／または記憶され、前記のシールドされた回路要素が保護領域と非保護領域間の非保護データおよび／または制御信号の転送を可能にするための論理回路要素を有する非保護領域を更に有する集積回路チップにおいては、シールドされた論理回路要素は第２の導電層により与えられる所定のパワー信号で動作する。この結果、保護データがチップの非保護領域に保護領域から伝達されるのを可能にするプローブのような手段により、制御手段が論理回路要素に送られるのを可能にするための第２の導電層の除去は、このような第２の導電層の除去または論理回路要素からパワーを除去するので、無益である。このような実施例において、前記のシールドされた複数の論理回路要素が夫々個別に第２導電層の重なった場所からのみ所定のパワー信号を受けるように論理回路要素と重った第２導電層のその場所にのみ別々に接続されている。

この発明の別の態様において、シールドされた回路要素は保護データを記憶するためのメモリと、そのメモリにデータが記憶されるようにする論理回路を有し、その第２導電層は論理回路のその機能にとって必要である信号を導く。この結果、チップの意図とした保護を損なうようにメモリ内で悪意のある内密データが保護データに入れ代わられるのを可能とする制御信号を論理回路に送るための第２の導電層の除去は、この第２の導電層の除去が論理回路によってメモリにデータが記憶されるのを妨げるので無益となるであろう。

（実施例）

第１図に於て、本発明の好ましい実施例である集積回路チップ10は保護領域11と非保護領域12と備えている。チップ10はVLSI（Very Large Scale Integrated）回路チップである。このチップ10は保護領域11内に次の回路要素を形成している。即ち、保護データを処理するマイクロプロセッサ14と、保護テータを記憶する複数のメモリ$M_1, M_2 \cdots M_n$と、保護データバス16と、保護アドレスバス17と、転送論理回路18と、保護クロック並びにパワー制御回路20とである。このチップ10はこのような回路要素の特定の組合わせである必要はなく、その中で保護データが無承諾の読み取り或は保護データおよび／または指令の変更に対し保護されているような回路要素のいかなる組合わせであってもよい。このメモリ$M_1, M_2 \cdots M_n$はどんなタイプでもよく、例えばRAM（ランダムアクセスメモリ）、ROM（読み取り専用メモリ）、EPROM（電気的書込可能な読み取り専用メモリ）、EEPROM（電気的消去書込可能な読み取り専用メモリ）等や、レジスタファイル

やFIFO（ファストイン／ファストアウト）バッファ等であっても良い。
導電層CN_2は回路要素14,M_1,M_2…M_n、16,17,18,20が外部から検知され得ない様にシールドするためにこれらの回路素子を上から覆っており、こうして保護領域11を形成している。
非保護領域12の中で、チップ10は次の如き回路要素を形成している。即ち、メモリ24と論理回路26と非保護データバス28とである。
MOS回路要素を有するチップ10の実施例では第２図と第３図とに示す如く、このチップは半導体基板層SCと第１絶縁層DE_1と、第１導電層CN_1と、第２絶縁層DE_2と、第２導電層CN_2と続き、第ｎ番目の絶縁層DE_nと、ｎ番目の導電層CN_nとを有する。半導体基板層SCの中の拡散部分ＳとＤは、ソースとドレンを形成し、それ等はゲート導体Ｇと組合され第１導電層CN_1により相互接続され、チップ10の回路要素を画成するように配列された相補性MOS電界効果トランジスタを形成している。第１導電層CN_1は第１絶縁層DE_1の孔を通る、導電性接触片30によりソースＳとドレンＤとに接続されている。第２導電層CN_2は第２絶縁層DE_2にある孔を通る、接触片31により、シールドされた回路要素の意図した機能に必要な所定の信号を回路要素に伝えるため第１導電層と接続されている。
第２導電層CN_2を除去するとこの回路要素に所定の必要な信号を伝えられなくなり、従って意図された機能も不可能になるであろう。第２導電層CN_2は回路要素を上から覆うことで、その中に回路要素が外部から検知され得なくなる様にシールドされている保護領域11を形成する。
バイポーラ回路要素を有するチップ10の実施例では、第４図に示す如く、このチップは半導体基板層SCと、第１絶縁層DE_1と、第１導電層CN_1と、第２絶縁層DE_2と、第２導電層CN_2と、第ｎ番目の絶縁層DE_nと、ｎ番目の導電層CN_nとを有している。半導体層SC内の拡散部ＣとＢとＥは、コレクタと、ベースと、エミッタとを形成し、これらは第１導電層CN_1により相互接続され、チップ10の回路要素を画成するように配列されたバイポーラトランジスタを形成している。第１導電層CN_1は第１絶縁層DE_1にある孔を通る、導電性接触片32により、シールドされた回路要素の意図した機能に必要な所定の信号を回路要素に伝えるため、コレクタＣとベースとに接続されている。第２導電層CN_2は第２絶縁層DE_2にある孔を通る接触片33により、シールドされた回路要素の意図した機能に必要な所定の信号を回路要素に伝えるため、第１導電層CN_1と接続されている。
第２導電層CN_2を除去すると、この回路要素に所定の必要な信号を伝えることが出来なくなり、従ってその意図された機能も不可能になるであろう。第２導電層CN_2は回路要素を上から覆うことで、その中に回路要素が外部から検知され得なくなる様にシールドされている保護領域11を形成する。
保護データを配分し記憶し処理し或は処理を実行するチップ10のすべての回路要素は、シールドとして機能して保護領域11の境界を形成する層CN_2の如き導電層より前に作られ、その下に位置する相互接続層CN_1の如き、導電層を利用している。
その下にある回路要素を動作不要にすることなしに除去出来ぬ第２導電層CN_2は機械的とSEM（走査型電気顕微鏡）のプロビングに対するシールドとしての機能と、所定の必要な信号を伝達する層としての機能とを有する。所定の必要な信号はパワー信号でも命令の如き制御信号でもよい。所定の必要な信号がパワー信号である場合検知の目的でのシールド層CN_2の除去は機械的であれ化学的であれ或いはその他の手段であれ下にある回路要素からパワーを処断することとなり動作不能にし更に多分同じ回路要素に記憶されている何らかのデータや論理状態を失わせることにもなるであろう。
この技術は、特に揮発性RAMの如き揮発性メモリに記憶されている保護データを守るのに有効である。その中のメモリM_1とM_2とが揮発性メモリであるチップ10の実施例に於て、このメモリM_1とM_2は夫々外部からの検知からシールドするため第２導電層CN_2により覆われている。そして、パワー信号は別々に夫々のメモリM_1,M_2と重っている第２導電層CN_2の部分から夫々のメモリM_1,M_2に分配される。この分配は第５図に示され、第２導電層CN_2は揮発性メモリの中のトランジスタのソースＳに、接触片34によりメモリにパワーを配分するために、接続されている。夫々のメモリM_1,M_2を検知するために第２導電層CN_2の重った部分を除去することは、夫々のメモリM_1,M_2からパワーを遮断することとなる。メモリM_1,M_2は揮発性であるからそこからパワーを遮断することはその中に記憶された保護データを消去することとなる。従ってメモリM_1,M_2の内容をそのメモリに重っている第２導電層CN_2の部分のみを除いて検知しようと試みても無駄であろう。
第６図に示した他の実施例に於て、パワー信号V_{cc}は第２導電層CN_2から複数の揮発性メモリ要素Ｍに前述の実施例よりも小さいスペースですむ方法で分配される。その中ではパワーはそのメモリ要素Ｍと重った第２導電層の部分のみからそのメモリ要素Ｍに別々に配分される。この実施例では夫々のメモリ要素Ｍの列は下にある別々の第１導電層CN_1を経由して重った第２導電層CN_2からパワーを受けとる。この第２導電層CN_2は夫々の第１導電層CN_1に導電性接触片35により接続されている。この実施例は面積効率を上げるため多少の安全性を失ってはいるがこれ等のメモリ要素Ｍを、すべての中間層接続導電性接触片35とそれにパワーを供給する第２導電層CN_2のその部分に触れないで、第２導電層CN_2の除去から起こるパワー遮断によるデータの消去を起こすことなしに検

知しようとすることは非常に高い分解精度のある第２導電層の除去が求められるであろう。
いかなる導電層の組合わせもこの実施例で使用されることができる。シールドする導電層としてチップの縦方向に最もしっかりと埋め込まれた導電層の使用は最大の安全性を生じる。
今一度第１図に於て、非保護領域12の中では論理要素26とメモリ24とは非保護データと制御信号を処理し記憶する。非保護データと制御信号は非保護データバス28から保護領域11にある保護データバス16に転送論理回路18により転送される。転送論理回路18は非保護データと制御信号をマイクロプロセッサ14により保護データと共に処理するために保護領域11にある保護データバス16に転送する。転送論理回路18は非保護データが保護データバス16にある時に示すマイクロプロセッサ14により起される制御信号に呼応して非保護データと制御信号が非保護データバス28と保護データバス16の間に転送され得るようにする。マイクロプロセッサ14は保護データバス16にあるデータ信号の状態をモニタし論理回路18が、データ信号と制御信号を非保護データバス28と保護データバス16の間に、非保護データが保護データバス16上にある間のみ転送可能とする制御信号を発生する。
上述の如く、導電層CN_2は転送論理回路18を外部からの検知からシールドする為に転送論理回路18に重っている。この導電層CN_2は又パワー信号を転送論理回路18に伝える。従って、転送論理回路18を検知する目的で導電層CN_2を除去することは転送論理回路18からパワーを遮断することになり転送論理回路18が何かのデータ或は制御信号を保護データバス16と非保護データバス28の間に転送することを妨げる。同様に制御信号を転送論理回路18に配ることを可能にするために保護データをチップ10内で保護領域11から非保護領域12に転送することができるプローブの如き手段により導電層CN_2を除去することは、シールドしている導電層CN_2もまた転送論理回路18からパワーを遮断するので無益なことであろう。
この技術は悪意のある内密のデータが非保護領域12から保護メモリ$M_1, M_2 \cdots M_n$に書き込まれることがないように逆方向にも拡張出来る。マイクロプロセッサ14は保護データバス16にあるデータをメモリ$M_1, M_2 \cdots M_n$に記憶出来るようにするメモリアクセス論理回路を備えており、シールドしている導電層CN_2はパワー信号をマイクロプロセッサ14に伝える。従って、制御信号をマイクロプロセッサ14のメモリアクセス論理回路を伝えるため、このことはメモリ$M_1, M_2 \cdots M_n$の中で悪意のある内密のデータを保護データに置き換えることが出来、従ってチップの予期された安全を危くすることとなるが、シールドしている導電層CN_2を所越することは、この除去がマイクロプロセッサ14からパワーを除き従ってメモリアクセス論理回路がメモリ$M_1, M_2 \cdots M_n$にデータを記憶させることをさまたげるから無益である。
１つの実施例に於ては保護領域内のシールドされた論理回路14,18は夫々別々にシールドしている導電層CN_2の重っている部分のみからパワー信号を受け取るためにその論理回路14,18に重っているシールドしている導電層CN_2の夫々の部分のみに接続されている。
第７図に示す実施例に於て、保護信号はシールド層CN_2とCN_nの下にある導電層CN_1に配分される。そしてシールド信号（必要な制御或いはパワー信号の如き）は上に覆っているシールド層CN_2とCN_nに別々に配分される。１つのシールドしている導電層CN_nの境界は図中では実線で示され、他のシールドしている導電層CN_2の境界は図中に破線で示され、下にある導電層CN_1は図中ボカしで示される。下にある導電層CN_1はシールドしている導電層CN_2とCN_nの１つの或は他のものにより完全にシールドされている。そして下にある導電層CN_1の１つの部分はシールドしている導電層CN_2とCN_nの両者によりシールドされている。
このシールド層CN_2とCN_nを化学的或は普通のレーザ或はマイクロプローブで導電層CN_1中の保護信号にアクセスするために切り開くと言う試みは導電層CN_1がシールド層CN_2とCN_nへ接続（短絡）されるか導電層CN_1とCN_2とCN_nで形成される回路パスの中にオープン回路が出来ることとなる。従って、保護信号と必要な信号の配分を混乱させ導電層CN_1とCN_2とCN_nに接続されている回路要素の意図した機能を変化させてチップ10の意図した機能を損なう。
チップ10に記憶されたある保護データがそのチップの入った製品の製造中にその保護データが記憶されたあとは変更されないということは極めて重要である。この目的を成就するため、チップ10は所定のメモリ位置に記憶された保護データの変更を妨げるためのシステムを有している。このような予防システムの他の実施例を第８図と第９図とに示す。
第８図のシステムはメモリＭと、メモリ制御論理回路38と、復号器40と、フューズ要素42と、フューズ変更素子44を有する。このシステムはメモリＭに適用されその中に保護データが記憶される夫々のメモリ$M_1, M_2 \cdots M_n$がメモリＭとして含まれている。
このメモリＭはデータバス16からの変更不能な保護データを記憶する所定の位置を含めて複数のメモリ位置を持っている。
メモリ制御論理回路38はアドレスバス46によりメモリＭに接続されて、“書込み”信号がメモリ制御論理回路38から保護メモリＭへのライン47上に与えられた場合データがアドレスバス46に与えられたアドレス信号により指示されたメモリＭの位置に記憶されるようにする。
フューズ要素42は最初の状態と非可逆的に変化した状態とを持っている。“フューズ要素”という言葉はフューズとアンチフューズとをいっている。フューズ要素はチップ10の中で金属性導電層とポリシリコンの導電層の組

合わせで形成される。アンフューズ要素はチップの中で金属性導電層或はポリシリコンの導電層或は両者の組合わせで形成され得る。アンチフューズ要素はチップの中の導体／酸化物導体構造或は導体／アモルファスシリコン／導体構造によりチップの半導体層の中に形成されるP^+/N^+半導体接合ダイオードとP^-/N^-半導体接合ダイオードとにより形成される。

フューズ変更素子44は保護領域11より外にある端子50からライン48に来る所定の制御信号に呼応してフューズ要素42の状態を非可逆的に変化させるためにフューズ要素42に接続されている。更にライン48の制御信号は保護領域11の内部にある端子（図示していない）から供給される。

復号器40はフューズ要素42の状態のアドレスバス46のアドレス信号をモニタするためと、所定のメモリ位置にアドレスバス46上のアドレス信号により示される時は何時でもフューズ要素42の状態が非可逆的に変更してしまったあとでメモリＭの所定のメモリ位置にデータが記憶されるようにするのをメモリ制御回路38が防ぐためにフューズ要素42とメモリ制御回路38とアドレスバス46とに接続されている。

第２導電層CN_2は、メモリＭとメモリ制御論理回路38と復号器40とフューズ要素42とを外部からの直接アクセスからシールドしている。

メモリＭとメモリ制御論理回路38と復号器40は第２導電層CN_2から来るパワー信号によって働かされるようにすべて第２導電層CN_2に接続されている。

第８図のシステムはメモリＭの所定の位置に最初から記憶された保護データの変更を防ぐのに使われる。フューズ要素42の状態が非可逆的に変化した場合、復号器40はアドレスバス46上のアドレス信号により示された所定のメモリ位置に何らかの追加データが書き込まれるのを防ぐ。

第８図のシステム中のフューズ要素42は又このチップを使っている製品がその使用者に届く時に先だってのみ適用出来るある予備的な保護データ処理機能、例えば保護データの予備的処理或は保護データを処理するインストラクションのローディングを行ったりそれに影響したりする他のシールドされた回路要素（図に示されていない）に接続されることもできる。復号器40の如き手段はフューズ要素をモニタするためと、フューズ要素の状態が非可逆的に変化してしまったあとでは他のシールドされた回路要素の予期された機能を保護するためにフューズ要素42と他のシールドされた回路要素に接続されている。

多くのフューズ技術は、保護集積回路チップの製造工程中工場でのみフューズすることを可能にする。例えば、ある工場は素子のよりよい長期信頼性を得るためにフューズが切れたあと、ポリシリコン（或は他のフューズ材料）上に酸化物を成長させることを要求している。第９図のシステムは、別の製造者が工場でのフュージングの後、保護メモリＭへ保護データを入力することを可能にしているが、保護メモリＭの内容の変更を妨げている。

第９図のシステムはメモリＭと、EPROM或はEEROM（電気的消去可能なROM）の如き消去可能なメモリ52と、メモリ制御論理回路54と、駆動回路55と、フューズ要素56と、ANDゲート57と、フューズ変更素子58とを有する。

メモリ制御論理回路54はANDゲート60と、ANDゲート60と消去可能なメモリ52とを結ぶインバータ62並びに配線を含むＮ接続とを備えている。インバータ62はANDゲート60への選ばれた入力と消去可能なメモリ52中の選ばれたメモリ位置との間に接続されて、ANDゲート60を働かせるには必要な消去可能メモリ52中に所定のデータパターンを形成する。

メモリＭは変更不能な保護データを記憶する所定の位置である複数のメモリ位置を持っている。

駆動回路55は、書込駆動信号がライン63を通じ駆動回路55に加えられたとき、消去可能メモリ52にデータパターンを記憶され得るようにする。

メモリ制御論理回路54は消去可能なメモリ52が所定のデータパターンを容れている時は何時でもライン64からANDゲート60への書込み信号に呼応して第１メモリＭの所定の位置にデータが記憶されるようにメモリＭと消去可能なメモリ52と接続されている。

消去可能なメモリ52の内容はチップ10の保護領域11の外部にある消去端子66から“消去”の制御信号が与えられることで消され得る。

フューズ要素56は、最初の状態と非可逆的に変化した状態とを持っている。フューズ変更素子58は保護領域11の外部にある端子68からライン67に与えられる所定の制御信号に呼応してフューズ要素56の状態を非可逆的に変化させるためにフューズ要素56に接続されている。或いはまたライン67の制御信号は保護領域11の内部にある端子（図示していない）から供給される。

データパターンはデータ端子69から供給されANDゲート57を通り消去可能なメモリに供給される。ANDゲート57はフューズ要素56が最初の状態にある間のみ消去可能メモリ52にデータを書込ませることが出来るようにフューズ要素56につながる１つの入力をもっている。

フューズ要素56は又フューズ要素56の状態が非可逆的に変化する前のみ消去可能なメモリ52に所定のデータパターンを記憶させられるように駆動回路55と接続されている。

消去可能なメモリ52はＮビットが必要である。工場では、消去可能なメモリ52とANDゲート60とに接続されたインバータ62のパターンに対応している所定の1,0のパターンが、ANDゲート60がライン64を通じメモリＭに“書込み”制御信号を送れるように、消去可能なメモリ52に入れられる。1,0の所定のパターンが消去可能なメモリ52に入れられたあと、フューズ要素56状態が非可逆

的に変化されると所定のパターンは変更出来なくされる。この点で集積回路チップ10の処理や包装は継続可能となり消去可能なメモリ52に記憶された所定のパターンを乱すことなく最終処理と包装が出来る状態になる。
チップ10が別の製造者に出荷されたあと保護データは保護メモリMに記憶され得る。それは消去可能なメモリ52記憶された所定のパターンが、インバータ62によりメモリ制御論理回路54にワイヤ結線で入れられた所定のパターンに適合しているからである。
一旦保護データが保護メモリMに記憶されると“消去”信号が消去可能なメモリ52の内容を消去するために消去端子66に加えられても保護メモリMの中に記憶された保護データは変化しない。第２導電層CN_2はメモリMと、消去可能なメモリ52と、メモリ制御論理回路54と、駆動回路55と、フューズ要素56とを直接的外部からのアクセスからシールドしている。
この技術は第９図のシステムをチップ10のカバー層を通し消去可能なメモリ52を遠くからプログラムし直せるような非常に正確なＸ線ビームや他の複雑な手段のいかなる攻撃の断片からも守ることが出来る。この技術の安全保障はEEROMやEPROMの内容を多くからプログラムし直すこと或いは切れたフューズを再接続することは困難だということに由っている。たとえ非常に強力な焦点を結ばない或いは発散性Ｘ線或は他の手段が、EEROM或はEPROMの内容を本質的に無作為化することが出来るとしても、攻撃者は駆動パターンを完成させる企てをくりかえることとなる。従って安全保障はEEROM或はEPROMのセルがこれ等の状態によって、言い換えれば、すべて１かすべて０かの好ましいパターンの方向にバイアスされるように設計されることも求め得る。従って何らかの焦点の結ばれないビームは高い確率でその内容をメモリMにデータを記憶される所定のパターンに対するよりはむしろ好ましいパターンに進ませ得る。安定度はより大きいビット数Ｎのより長い所定のパターンを使用することで増加させる。
メモミMと消去可能なメモリ52とANDゲート60と駆動回路55とはすべて第２導電層CN_2に接続され、第２導電層CN_2により運ばれるパワー信号により加勢される。
第９図に示すシステムのフューズ要素56は、保護データの或る前記処理機能を果たす或いはそれを実行する他のシールド回路要素（図示せず）に接続され得る。保護データの前処理或は保護データの処理のための指示を加えるような前処理機能は、チップを含むこの製品がこの製品の使用者に渡る前にのみ適用できる。フューズ要素56は、フューズ要素56の状態が非可逆的に変更される前にのみ、他のシールド回路要素の意図した機能が果たせるように、他のシールド回路要素に接続される。
第８図並びに第９図に示す保護データ変更防止システムは、“Prevention of Alternation of Data Stored in Secure Integrated Circuit Chip Memory”と題する、同日に出願された本願の関連出願の主題である。
複雑な集積回路チップの製造は、含まれる全ての回路素子が正確に動作することを確かめるためのテスト操作の間、内部回路素子への完全なアクセスを必要とする。しかし、テストのための高いアクセス可能性は、一般に保護データもしくは変更されてはならないデータを含むチップに対しては安全上弱点となる。
第10図は、テスト動作が完了した後に、テスト信号パスを永久的に無能にし、この結果チップの外部ピンからの内部保護データ回路要素へアクセスをもはや不可能にするシステムを示す。このシステムはフューズ要素70と、第１並びに第２のインバータ72,74と、抵抗75と、第１並びに第２のNANDゲート76,78と、フューズ変更素子79とを有する。
前記フューズ要素70は最初の状態と、非可逆的に変化した状態とを有する。フューズ変更素子79はフューズ要素70に接続され、保護領域11の外部の端子81からライン80に受信する所定の制御信号に応答して、フューズ要素70の状態を非可逆的に変化させる。或いはまた、ライン80の制御信号は保護領域11の内部の端子（図示せず）から受信される。このフューズ要素70は第１および第２のNANDゲート76,78に接続されて、チップ10の保護領域がフューズ要素70の状態が非可逆的に変化される以前にのみテストのためにアクセスされ得るようにする。
前記フューズ要素70とインバータ72,74とは直列にされ、第１のNANDゲート76への１つの入力に接続されている。この第１のNANDゲート76の出力信号は外部テストデータ出力端子82に印加される。
前記フューズ要素70とインバータ72,74とは直列にされ、また第２のNANDゲート78の出力端子の１つの入力に接続される。
前記第２のNANDゲート78は、チップ10の保護領域11内のテスト指令入力ノード86へ外部テスト指令入力端子84からのテスト指令信号を通す。テスト指令入力信号がテスト指令入力ノード86に与えられるのに応答して、テストデータがチップ10の保護領域11内の内部のテストデータ出力ノード88に与えられる。内部テストデータ出力端子に与えられるテストデータは、回路要素14,M_1,M_2…M_n,16,17,18,20（第１図に示す）のようなチップ10の保護回路要素からアクセスされ得る。
前記テストデータは、フューズ要素70が最初の状態のときにのみ、テストデータ出力ノード88から、第１のNANDゲート76を介して、外部テストデータ出力端子82に与えられる。
また、テスト指令入力信号は、フューズ要素が最初の状態の時にのみ、外部テスト指令入力端子84から内部テスト指令入力ノード86に与えられる。
前記第２の導電層CN_2は、直接的な外部アクセスから、フューズ要素70と、インバータ72,74と、抵抗75と、NANDゲート76,78とをシールドする。

前記インバータ72,74と、抵抗75と、NANDゲート76,78とは、全て第２の導電層CN_2に接続され、第２の導電層CN_2からのパワー信号により加勢される。

プローブによる攻撃を防止するように、可能な限りチップ10内に深く、フューズ要素70から第１並びに第２のNANDゲート76,78への信号通路を埋め込むことにより、付加的保護がなされる。かくして、フューズ要素70から第１並びに第２のNANDゲート76,78への信号通路は、主としてN^+,P^+拡散部内に形成される。同様により低い安全性で、ポリシリコン並びに他の導電層が使用され得る。最上の導電層CN_n,CN_{n-1}の使用は避けるべきである。

【図面の簡単な説明】

第１図は本発明による集積回路チップのブロックダイヤグラム。

第２図は本発明による集積回路チップにおけるMOS回路要素のシールディングを示す断面図。

第３図は回路要素をシールドし、シールドされたMOS回路要素へ所定の信号を送る重った導電層を示す平面図。

第４図は本発明の集積回路チップにおけるバイポーラ回路要素のシールディングを示す断面図。

第５図は回路要素はシールドし、シールドされた回路要素に電力を供給するための重った導電層を示す断面図。

第６図は複数の揮発性メモリをシールドしている別の実施例のブロックダイヤグラム。

第７図は回路要素の機能へ必要な信号を送る重った導電層を示す平面図。

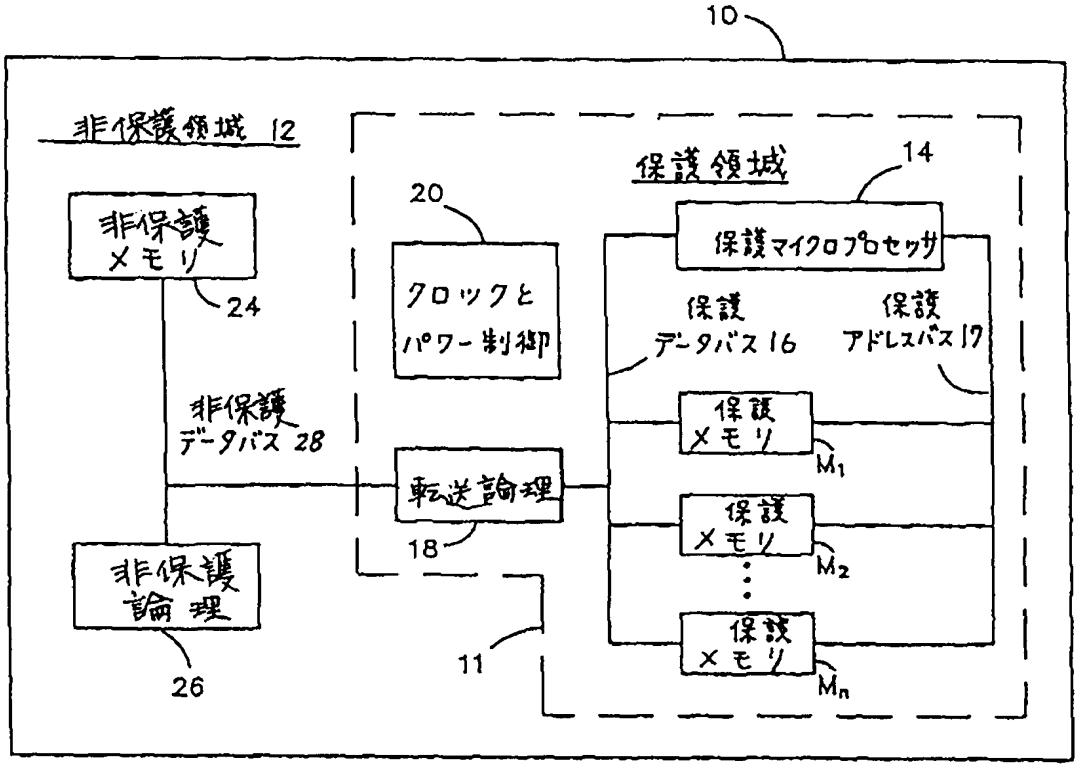
第８図はチップの保護領域内で所定のメモリ位置に記憶された保護データを変更することを妨げるシステムの１つの実施例のブロックダイヤグラム。

第９図はチップの保護領域内で所定のメモリ位置に記憶された保護データの変更を防ぐシステムの別の実施例のブロックダイヤグラム。

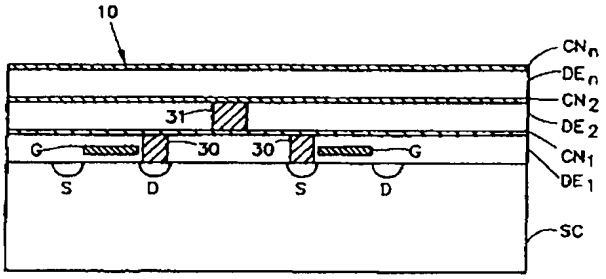
第10図は保護領域がテストのためにアクセスされ得る時に制限を加えるチップ内保護領域でのシステムの好ましい実施例のブロックダイヤグラム。

10……チップ、11……保護領域、14……マイクロプロセッサ、M_1,M_2…M_n……メモリ、16……保護データバス、17……保護アドレスバス、18……転送論理回路、20……パワー制御回路、SC……半導体基板層、DE_1……第１絶縁層、CN_1……第１導電層、DE_2……第２絶縁層、CN_2……第２導電層、S,D……拡散部分。

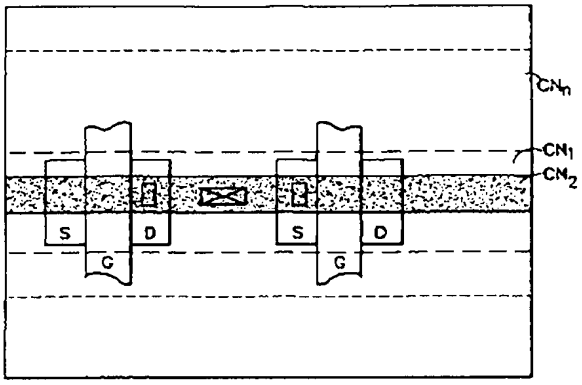
【第１図】



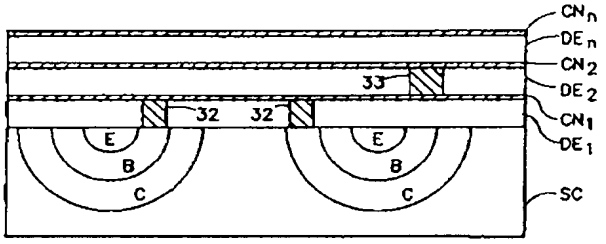
【第２図】



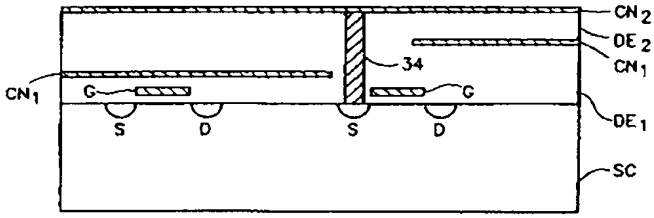
【第３図】



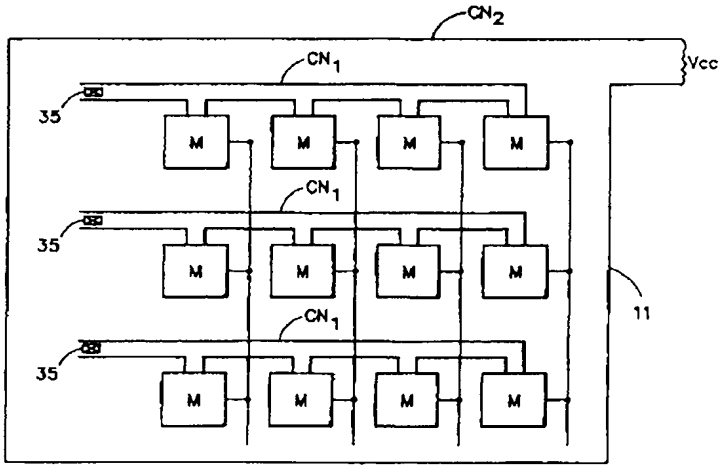
【第４図】



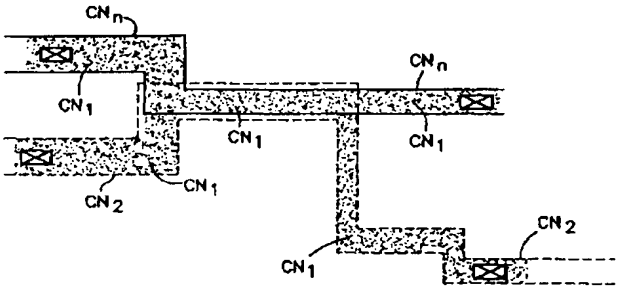
【第５図】



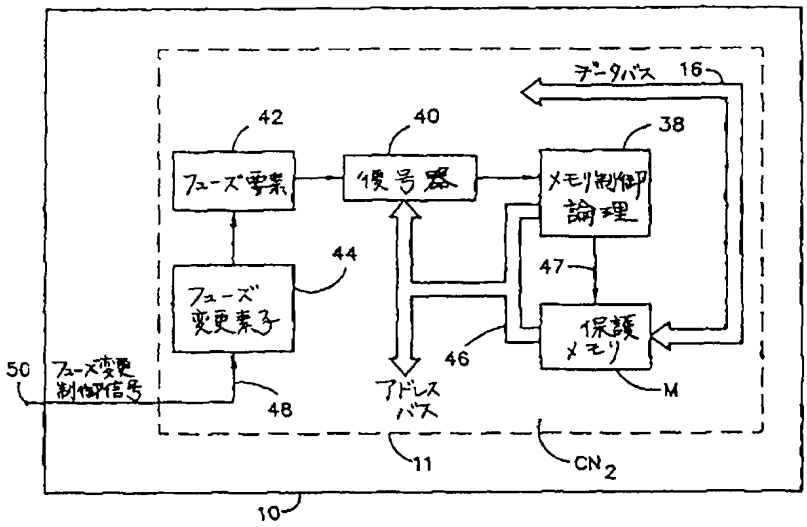
【第６図】



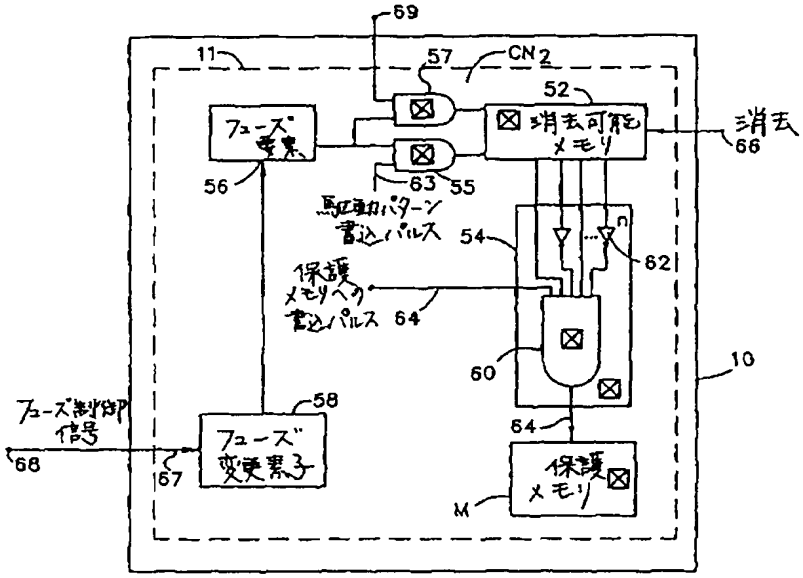
【第７図】


CNn
CN1
CN2

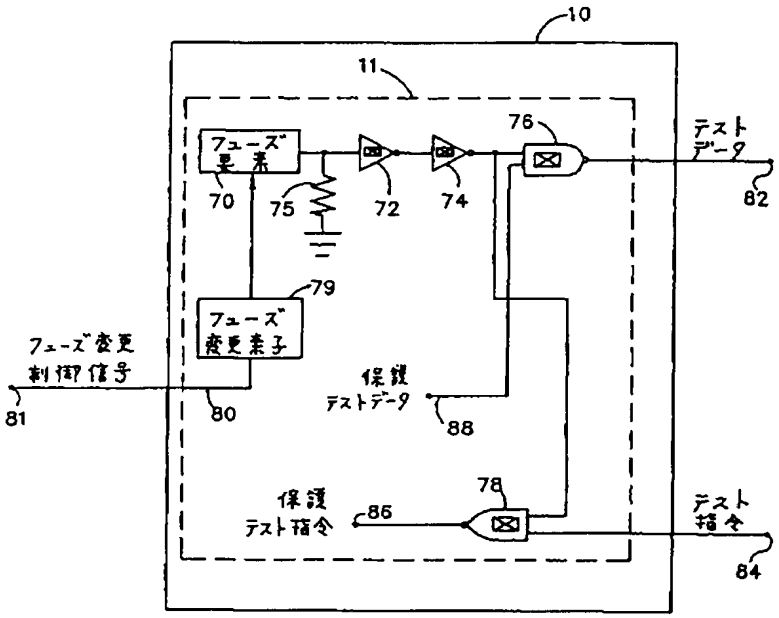
【第８図】


データバス
16
42
40
38
フューズ要素
復号器
メモリ制御論理
44
47
フューズ変更素子
保護メモリ
50
フューズ変更制御信号
48
46
アドレスバス
M
11
CN2
10

【第９図】


69
11
57
CN2
52
フューズ要素
消去可能メモリ
消去
66
56
63
55
駆動パターン書込パルス
54
n
62
保護メモリへの書込パルス
64
60
10
フューズ制御信号
58
68
67
フューズ変更素子
64
保護メモリ
M

【第１０図】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
ＨＯ１Ｌ　21/8247				
29/788				
29/792				
		8832－4M	ＨＯ１Ｌ　21/82	Ｄ

(72)発明者　ポール・マロニー
アメリカ合衆国、カリフォルニア州　92007、カーデイフー　バイー　ザー　シー、アボセット・コート　1249

(72)発明者　ウイリアム・アレン・シュメイト
アメリカ合衆国、カリフォルニア州　92116、サンデイエゴ、ビオナ・プレイス　4202